UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/809,599	03/25/2004	Huayan Amy Wang	A35947 - 072797.0222	7239

21003 7590 06/28/2006

BAKER & BOTTS
30 ROCKEFELLER PLAZA
44TH FLOOR
NEW YORK, NY 10112

EXAMINER	
DAVIS, ZACHARY A	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 06/28/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/809,599	WANG, HUAYAN AMY	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Specification

1. The disclosure is objected to because of the following informalities:

On page 5, in paragraph 0016, the disclosure states that IEEE Standard 802.11 is incorporated by reference; however, it is not clear which version of the standard, or the standard as of what date, is to be incorporated into the disclosure of the present application.

Further, the specification appears to contain minor typographical and other errors. For example, on page 7, in line 8 of paragraph 0019, it appears that "the analysis described are preferably performed" is intended to read "the analysis described is preferably performed"; in lines 16-17 of page 9 (within paragraph 0023), it appears that "packets received in the future may checked" is intended to read "packets received in the future may be checked"; in line 1 of page 10 (within paragraph 0024), the phrase "the source MAC address may be extracted may be checked for any suspicious settings" is generally unclear; on page 11, in line 7 of paragraph 30, it appears that the right parenthesis should be removed after "length"; and on page 13, in lines 2-3 of paragraph 0039, it appears that "may be categorizes" is intended to read "may be categorized".

Appropriate correction is required. The above is not intended as an exhaustive list of errors. Applicant's cooperation is requested in correcting any other errors of which applicant may become aware in the specification.

Claim Objections

2. Claims 23 and 36 are objected to because of the following informalities:

It appears that Claim 23 is intended to depend from Claim 19, instead of Claim 18 as written.

It appears that Claim 36 is intended to depend from a claim other than Claim 1, as written. It is assumed that Claim 36 is intended to depend from Claim 19.

Appropriate correction is required.

3. Applicant is advised that should claim 18 be found allowable, claim 36 will be objected to under 37 CFR 1.75 as being a substantial duplicate thereof. When two claims in an application are duplicates or else are so close in content that they both cover the same thing, despite a slight difference in wording, it is proper after allowing one claim to object to the other as being a substantial duplicate of the allowed claim. See MPEP § 706.03(k).

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 3-9, 12-17, 21-35, and 38 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 3-7, 21-25, and 38 recite the limitation "IEEE Standard 802.11". This renders the claims indefinite, because the standard has been subject to revisions, and it is not clear to which version of the standard the claimed limitation is intended to be directed. Because the standard is evolving, such broad identification of the standard cannot be used to properly identify the specific methods, systems, or protocols associated with the standard, and therefore the scope of the claims is uncertain.

Claims 13 and 31 each recite the limitation "checking a More Data field of said received data packets". This is generally vague. It is not clear what, exactly, the field is checked for.

Claims not specifically referred to above are rejected due to their dependence on a rejected base claim.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1-39 are rejected under 35 U.S.C. 102(e) as being anticipated by Macaulay, US Patent Application Publication 2003/0135762.

In reference to Claim 1, Macaulay discloses a method for detecting unauthorized attempts to access a wireless data communication system, where the method includes forwarding one or more packets received by an access point to a computer that compares the format of the packets to a format specified by a protocol (see paragraphs 0045-0046 and 0095-0107; note also paragraphs 0032-0035 and 0042 where the wireless network is monitored), and signaling an alert if the packets deviate from the protocol specified format (see paragraphs 0049-0050).

In reference to Claim 2, Macaulay further discloses a header message portion and comparing the format of the header portion to the protocol specified format (see the table following paragraph 0094).

In reference to Claim 3, Macaulay further discloses that the protocol is IEEE Standard 802.11 (see, for example, paragraph 0002).

In reference to Claims 12-15 and 17, Macaulay further discloses monitoring for a possible denial of service attack (paragraph 0106) and that the packets may contain unsupported values and lengths (paragraph 0107, for example).

In reference to Claim 4, Macaulay further discloses comparing format of a frame control field (see the table following paragraph 0094).

In reference to Claims 5 and 6, Macaulay further discloses IEEE Standard 802.11 Management and Control frames (see the table following paragraph 0094; see also paragraph 0099).

In reference to Claims 7 and 8, Macaulay further discloses comparing a WEP flag value (see paragraph 0104).

In reference to Claim 9, Macaualay further discloses a protocol version (see, for example, paragraph 0083).

In reference to Claims 10 and 11, Macaulay further discloses source MAC addresses that are multicast and broadcast addresses (see paragraphs 0124, 0127).

In reference to Claim 16, Macaulay further discloses detecting a spoofed MAC address (paragraphs 0095, 0101).

In reference to Claim 18, Macaulay further discloses maintaining a state table in the computer (see paragraphs 0043-0046; 0090; 0101-0102).

In reference to Claim 19, Macaulay discloses a method for detecting unauthorized attempts to access a wireless data communication system, where the method includes forwarding one or more packets received by a mobile unit to a

computer that compares the format of the packets to a format specified by a protocol (see paragraphs 0045-0046 and 0095-0107; note also paragraphs 0032-0035 and 0042 where the wireless network is monitored), and signaling an alert if the packets deviate from the protocol specified format (see paragraphs 0049-0050).

Claims 20-36 recite limitations similar to those recited in Claims 2-18, and are rejected by a similar rationale.

In reference to Claim 37, Macaulay discloses a method for detecting unauthorized attempts to access a wireless data communication system, where the method includes forwarding one or more packets received by a mobile unit to a computer that compares portions of the packets to a values stored in a state table according to a specified protocol (see paragraphs 0045-0046 and 0095-0107; note also paragraphs 0032-0035 and 0042 where the wireless network is monitored), and signaling an alert if the portions of the packets deviate from the stored values (see paragraphs 0049-0050).

In reference to Claim 38, Macaulay further discloses that the specified protocol is IEEE Standard 802.11 (see, for example, paragraph 0002).

In reference to Claim 39, Macaulay further discloses maintaining a state table in the computer (see paragraphs 0043-0046; 0090; 0101-0102).

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Hrastar, US Patent 7042852, discloses a system performing intrusion detection on an access point wireless network that includes protocol-based, signature-based, anomaly-based, and policy-deviation-based testing.

b. Aaron et al, WIPO Publication WO03/083659, discloses a system using anomaly detection for intrusion detection purposes on wireless networks.

c. Zhang et al, "Intrusion Detection in Wireless Ad-Hoc Networks", discloses a system using anomaly detection and other techniques for intrusion detection in wireless networks.

d. Internet Security Systems, "Wireless LAN Security: 8011.b and Corporate Networks", discloses potential attacks on wireless networks and recommends techniques for avoiding the attacks.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

zad

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER